EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. Authorization for this examiner's amendment was given in a telephone interview with the applicant representative, Mr. Alan W. Young (Reg. No. 37,970) on 10/28/10. During the telephone conference, Mr. Miller has agreed and authorized examiner to amend claims 17-25 to overcome the minor informalities and cancel the withdrawn claims 1-16, 82, 84-90.

3. In the Claims:

Please cancel claims 1-16, 82, 84-90.

Please replace claim 17 as follows:

17. A method for a network connected gaming system to prevent unauthorized software components of constituent computers of the gaming system from executing, the gaming system including a plurality of gaming machines each having a plurality of executable software components, the method comprising the steps of:

producing a separate and unique PKI certificate for each of the plurality of executable software components subject to receiving certification within each gaming machine, each software component subject to receiving certification including a unique identifier;

code signing each executable software component subject to receiving certification with its respective separate and unique PKI certificate, each respective PKI certificate being uniquely identified at least by a unique identifier that is uniquely associated with the executable software component such that identical executable software components in different ones of the plurality of gaming machines of the network connected gaming system are associated with identical identifiers and are code signed with identical PKI certificates, such that non-identical executable software components in different ones of the plurality of gaming machines are associated with separate and different identifiers and are code signed with separate and different PKI certificates and such that no two non-identical executable software components in different gaming machines are code signed with a same PKI certificate, and

configuring a software restriction policy certificate rule for each of the plurality of executable software components and enforcing, using a processor, each of the software restriction policy certificate rules to allow execution of only those executable software components whose code signed PKI certificate is determined to be authorized.

Please replace claim 18 as follows:

18. The method according to claim 17, further comprising the step of configuring software restriction policy rules to prevent execution of unauthorized software components.

Please replace claim 19 as follows:

19. The method according to claim 17, further comprising the step of configuring software restriction policy miles to prevent execution of all not explicitly authorized software components.

Please replace claim 20 as follows:

20. A method for a network connected gaming system to enable only authorized software components of constituent computers of the gaming system, to execute, comprising the steps of:

code signing each authorized software component with a PKI certificate such that identical authorized software components in different ones of the constituent computers are code signed with identical PKI certificates, such that non-identical authorized software components in different ones of the constituent computers are code signed with separate and different PKI certificates and such that no two non-identical authorized software components in different ones of the constituent gaming machines, are code signed with a same PKI certificate;

configuring a separate software restriction policy for each authorized software component in each of the constituent computers of the gaming system, and associating the configured separate software restriction policy with the PKI certificate with which the authorized software component was code signed;

enforcing, using a processor, the associated software restriction policy for each code signed authorized software component such that each code signed authorized software component in each of the constituent computers of the gaming system must be authorized to run by its associated separate software restriction policy.

Please replace claim 21 as follows:

21. The method according to claim 20, wherein the authorized software components are mandated by a regulatory body.

Please replace claim 22 as follows:

22. A method for a network connected gaming system to enable only authorized software components of constituent computers of the gaming system to execute comprising the steps of:

configuring a separate and unique certificate software restriction policy for each authorized executable software component of each, of the constituent computers of the gaming system such that the each authorized executable software component in each of the constituent computers of the gaming system must be authorized to run by its associated separate software restriction policy;

code signing each authorized software component with a PKI certificate such that identical, authorized software components in different ones of the constituent computers are code signed with identical PKI certificates, such that non-identical authorized software components different ones of the constituent computers are code signed with separate and different PKI certificates and such that no two non-identical authorized software components in different ones of the constituent gaming machines are code signed with a same PKI certificate;

configuring a first path software restriction policy to prevent unauthorized software components from executing;

configuring a second path software restriction policy to prevent non-explicitly authorized software components from executing;

enforcing the certificate software policy configured for each of the code signed authorized executable software components of each of the constituent computers of the gaming system, and

enforcing, using a processor, the first path software restriction policy and the second path software restriction policy.

Please replace claim 23 as follows:

23. The method according to claim 22, wherein the authorized software components are mandated by a regulatory body.

Please replace claim 24 as follows:

24. A method for a network connected gaming system to enable only authorized software components of constituent computers of the gaming system to execute, the gaming system including a plurality of gaming machines each having a plurality of executable software components the method comprising the stops of:

producing a separate and unique PKI certificate for each of the plurality of executable software components within the gaming system subject to receive certification, each respective PKI certificate being associated with a unique identifier that is uniquely associated with the executable software component such that identical executable software components in different ones of the plurality of gaming machines of the network connected gaming system are associated with identical identifiers and are code signed with identical PKI certificates, such that non-identical, executable software components in different ones of the plurality of gaming machines are code signed with separate and different PKI certificates and such that no two non-identical executable software components in different gaming machines are code signed with a same PKI certificate;

code signing each software component subject to receive certification with its respective separate and unique PKI certificate;

configuring a certificate software restriction policy for each of the respective separate and unique PKI certificate, and

enforcing, using a processor, the certificate software restriction policy for each of the respective separate and unique PKI certificates.

Please replace claim 25 as follows:

25. A method for downloading authorized executable software components and allowing execution of down, loaded authorized executable software components of a plurality of gaming machines of a network connected gaming system comprising the steps of:

for each of the plurality of gaming machines of the network connected gaming system:

code signing each authorized executable software component with a separate PKI certificate that is unique to the authorized software component such that identical executable software components in different ones of the plurality of gaming machines of the network connected gaming system are code signed with identical PKI certificates, such that non-identical authorized software component in different ones of the plurality of gaming machines are code signed with separate and different PKI certificates and such that no two non-identical authorized software components in different gaming machines are code signed with a same PKI certificate;

packaging the code signed authorized software components into an installation, package;

configuring install policies to install each code signed authorized executable software component contained in the installation package;

configuring certificate rule policies to allow execution of the installed code signed authorized executable software component;

configuring, using a processor, enforcement of the install policies and certificate rule policies.

Response to Arguments

4. Applicant's arguments (Appeal Brief – pages 22-43), filed 08/20/10, with respect to Claims 17, 20, 22, 24, 25 have been fully considered and they are persuasive.

Allowable Subject Matter

5. Claims 17-25 are allowed and renumbered 1-9.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to NIRAV PATEL whose telephone number is (571)272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nirav Patel /
Examiner, Art Unit 2435

/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435